US006268789B1

US 6,268,789 B1

(12) **United States Patent** (10) Patent No.: **US 6,268,789 B1**

Diamant et al. (45) Date of Patent: *Jul. 31, 2001

(54) **INFORMATION SECURITY METHOD AND APPARATUS**

(75) Inventors: **Erez Diamant**, Herzelia; **Amir Prescher**, Ramat Gan, both of (IL)

(73) Assignee: **Voltaire Advanced Data Security Ltd.**, Hertzlia (AU)

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **08/804,972**

(22) Filed: **Feb. 20, 1997**

Related U.S. Application Data

(63) Continuation-in-part of application No. 08/754,871, filed on Nov. 22, 1996, now Pat. No. 5,969,632.

(51) **Int. Cl.**[7] **H04Q 1/00**
(52) **U.S. Cl.** **340/5.74**; 713/200
(58) **Field of Search** 340/825.31, 825.34, 340/5.74; 395/186; 709/225; 713/200, 201, 202; 710/8, 10, 14, 36, 200; 711/163, 164

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,498,716	2/1985	Ward .
4,769,833	9/1988	Farleigh et al. .
4,799,153	1/1989	Hann et al. .
4,962,449	10/1990	Schlesinger .
4,975,950	12/1990	Lentz .
5,128,995	7/1992	Arnold et al. .
5,144,659	9/1992	Jones .
5,144,660	9/1992	Rose .
5,191,583	3/1993	Pearson et al. .

5,202,997	4/1993	Arato .
5,268,960	12/1993	Hung et al. .
5,289,540	2/1994	Jones .
5,317,746	5/1994	Watanabe .
5,343,525	8/1994	Hung et al. .
5,355,489	10/1994	Bealkowski et al. .
5,361,359	11/1994	Tajalli et al. .
5,384,854	1/1995	Downs et al. .
5,414,844	5/1995	Wang .
5,434,562	7/1995	Reardon .
5,463,632	10/1995	Tremblay .
5,475,839	12/1995	Watson et al. .
5,499,334	3/1996	Staab .
5,509,120	4/1996	Merkin et al. .
5,530,455	6/1996	Gillick et al. .
5,537,540	7/1996	Miller et al. .

(List continued on next page.)

OTHER PUBLICATIONS

Microsoft Power PointTools, Chapter 12, p.443, Library of Congress Catalog Card No. 934–70074.
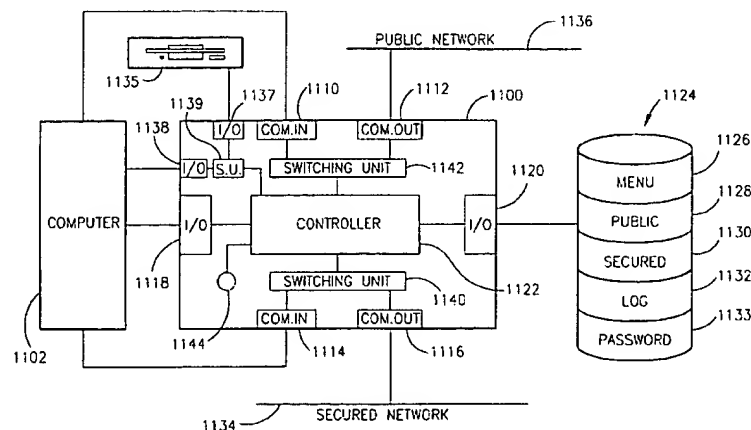
Primary Examiner—Edwin C. Holloway, III
(74) *Attorney, Agent, or Firm*—Eitan, Pearl, Latzer & Cohen-Zedek

(57) **ABSTRACT**

A device for protecting secured areas in a computer system which includes at least one storage unit divided into at least two storage areas. The device includes input-output (I/O) interfaces for connecting between the computer system and the storage unit, a managing controller connected to the I/O interfaces and communication interfaces connected to the managing controller, for linking between the computer system and communication networks. The managing controller provides the computer system with a selection between at least two modes. In each mode, the managing controller provides access to and from the computer to selected storage areas and communication networks. Furthermore, in each mode, the managing controller denies or provides limited access to and from the computer to non-selected storage areas and communication networks.

13 Claims, 14 Drawing Sheets

U.S. PATENT DOCUMENTS

Patent Number	Date	Inventor
5,542,044	7/1996	Pope .
5,559,883	9/1996	Williams .
5,564,002	10/1996	Brown .
5,570,367	10/1996	Ayanoglu et al. .
5,694,472	12/1997	Johnson et al. .
5,778,443	7/1998	Swanberg et al. .
5,815,571	9/1998	Finley .
5,896,499	4/1999	McKelvey .
5,909,586	6/1999	Anderson .
5,913,037	6/1999	Spofford et al. .
5,923,757	7/1999	Hocker et al. .
6,108,785	8/2000	Poisner .

FIG.1

FIG.2

FIG.3

PUBLIC
NETWORK

6

21

COMMUNICATION
INTERFACE

28

SWITCHING
UNIT

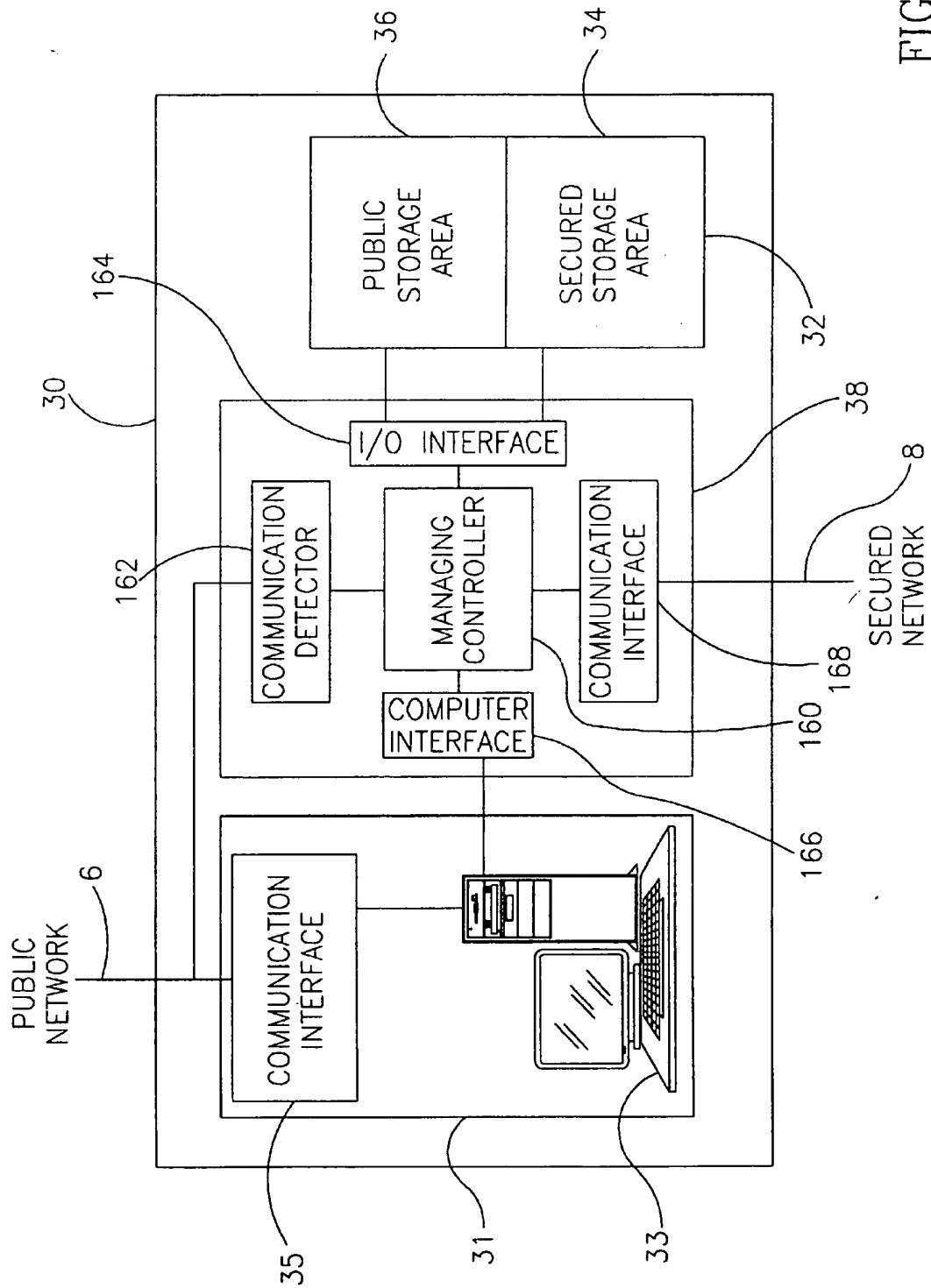COMMUNICATION
INTERFACE

SECURED
NETWORK

8

150

152

154

PUBLIC STORAGE
AREA

26

SECURED STORAGE
AREA

24

22

20

FIG.4

FIG.5

FIG.6

FIG.7

500 ── SET SECURITY FLAG OFF

502

DENY ACCESS ←── YES ── ON-LINE ?

504

NO   507

SECURITY FLAG ON ? ── NO

YES

GENERATE LOG FILE & SET SECURITY FLAG ON

506

GENERATE SECURITY KEY   508

RETRIEVE ANTI-VIRUS AND PROVIDE SECURITY KEY FOR C.P.U.   510

512   514

INFECTED ? ── NO ──→ ENABLE ACCESS

YES

ALERT   516

FIG.8

FIG.9

COMMUNICATION NETWORK

660

658

656

654

652

COMMUNICATION INTERFACE

STORAGE UNIT

COMMUNICATION DEVICE

650   COMPUTER

662 672 668

SWITCHING UNIT

664

666

PROCESSOR

STORAGE UNIT

670

FIG.10

FIG.11

DATA
BUS

CONTROLLER

LOG ENTRY
LOG ENTRY
LOG ENTRY
LOG ENTRY
LOG ENTRY

STORAGE AREA

1006

1004

1002

LOG UNIT

FIG.12   1000

RECEIVE A LOG
COMMAND   1050

1052

WRITE   WRITE : READ
COMMAND   READ

1054

1056

NO   Δt ≥ T   YES

RETRIEVE THE
REQUESTED
LOG ENTRY

1058

DENY ACCESS

RETRIEVE LOG
INFORMATION   1060

PROVIDE LOG
ADDRESS   1062

FIG.13

WRITE LOG
ENTRY   1064

FIG.14

DETECT BOOT ———1150

EXECUTE "MENU" ———1152

1154

USERS CHOICE OR TIME TIME OVER

S OR t>T   P

LOAD SECURED ———1162   1156——— LOAD PUBLIC

UPDATE SECURED FLAG ———1164   1158 UPDATE PUBLIC FLAG

1166 DETECT SWITCH   1160 DETECT SWITCH

SHUT DOWN SYSTEM
1168———

1170——— BOOT

———1172

PUBLIC ON   FLAG   SECURED ON
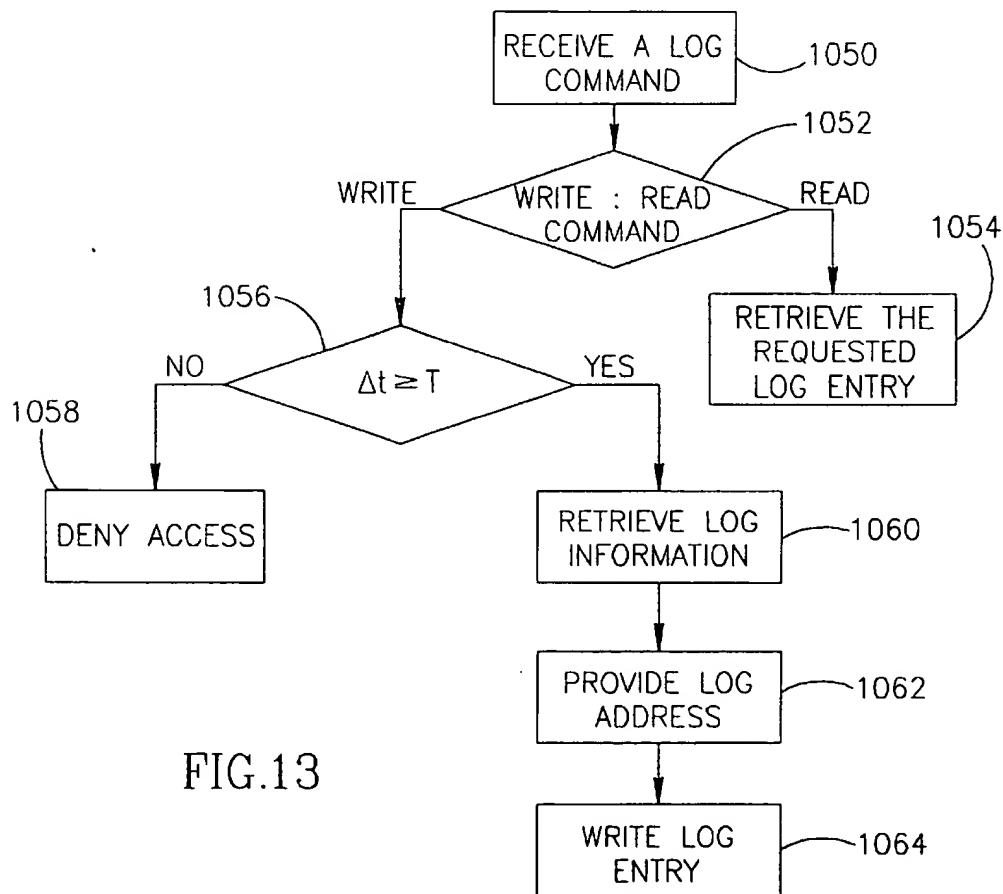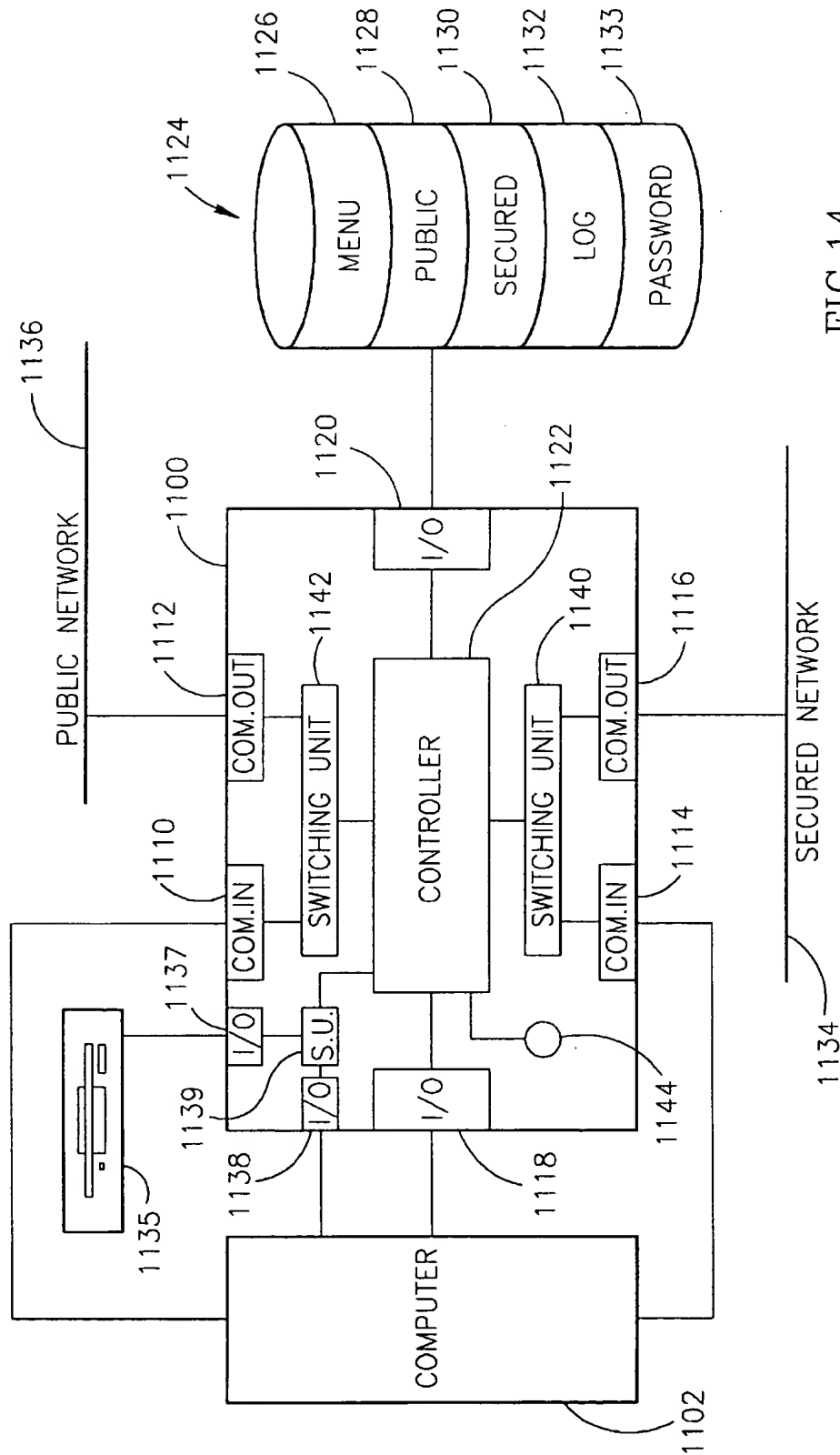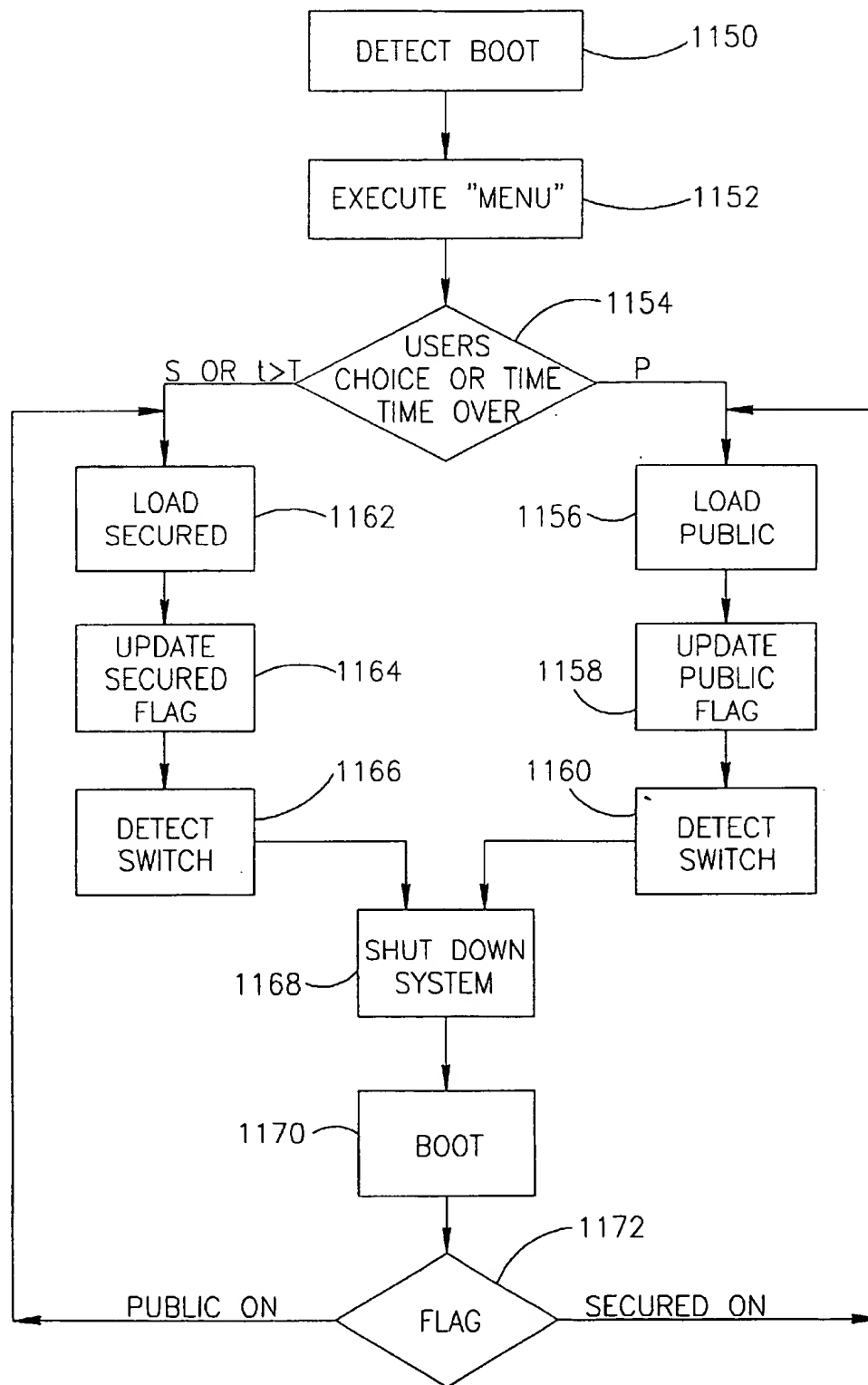
FIG.15

1

INFORMATION SECURITY METHOD AND APPARATUS

This is a continuation-in-part application of application Ser. No. 08/754,871, filed Nov. 22, 1996 now U.S. Pat. No. 5,969,632.

FIELD OF THE INVENTION

The present invention relates to methods and systems for securing information during communication.

BACKGROUND OF THE INVENTION

Method for securing information are known in art. Conventional methods are based on encryption wherein secured data is processed according to a predetermined encryption method or key to provide an encrypted file. Decoding the encrypted file, back to the original information requires processing the encrypted file backwards according to the encryption method or key.

Computers which are connected to WAN or LAN communication networks are vulnerable to hostile intrusion by unauthorized persons or data viruses which attempt to access classified files, download them and "crack" their encryption.

The problem is significantly enhanced for portable computers. Which are also liable to be stolen along with the information contained therein.

Another major problem relates to securing access to data and devices when in communication over a network. Unauthorized network users may attempt to penetrate the secured system or try to send damaging software, such as software viruses. Prior art software systems such as fire-walls and the like, do not provide a full proof solution against such unauthorized attempts.

Another major problem relates to securing an organization's networks and computers against virus programs. A number of products currently provide on-line scanning of incoming communication to identify damaging software such as viruses (such as WebShield of Finjan Software Ltd. of Netania, Israel, PCFireWall and WebScan of McCafee Inc. of Santa Clara Calif.). It will be appreciated that scanning all incoming data and data changes during communication consumes a great deal of resources and is generally not performed at a full scale in real time.

U.S. Pat. No. 5,434,562 to David C. Reardon describes a manually user operable switch for securing a device such as a hard disk from unauthorized access from a network.

In computer systems, it is common to implement an audit log, to record security related activities in the system. In this case, the recorded log itself needs to be secured against future alteration, which will deceive the auditor to trust a forged record.

It will be appreciated that an effective security log needs to be written on a media which cannot be altered. A common method is to print the log on hard copy. While hard copy is difficult to alter, it is also more difficult to duplicate, process and communicate in a computerized environment.

Another method is to write the log on a Write Once Read Many media (such as Pinnacle RCD-1000, Pinnacle Micro Corporation). It will be appreciated that in practice Write Once Read Many data storage solutions are inferior to common read-write technologies (such as magnetic hard disks) in both performance and reliability. Furthermore, the installation of a Write Once device for the sole purpose of recording a log involves significant costs.

SUMMARY OF THE PRESENT INVENTION

It is an object of the present invention to provide a novel device for securing access to and from a computer station, which overcomes the disadvantages of the prior art.

2

It is a further object of the present invention to provide a novel method for securing information contained in a computerized storage unit.

There is thus provided in accordance with the present invention a device for protecting secured areas in a computer system. The computer system includes a storage unit. The storage unit includes a first storage area and a second storage area.

The device of the invention includes a first communication interface for connecting to a first network, a second communication interface for connecting to the computer system, a first input-output (I/O) interface for connecting to the storage unit, a second input-output (I/O) is interface for connecting to the computer system, a managing controller connected between the first network and the computer system via the first and second communication interfaces, the managing controller also being connected between the storage unit and the computer system via the first and second I/O interfaces.

The managing controller provides the computer system with a selection between at least two modes. In a first mode, the managing controller connects the computer system to the first storage area and to the first network and in a second mode, the managing controller connects the computer system to the second storage area.

The managing controller detects any reset signal followed by a command to operate according to a selected mode, which may be provided either by a user, operating the computer system or by a software application.

According to one aspect of the present invention, the device may further include a third communication interface for connecting to a second network and a fourth communication interface for connecting to the computer system. According to this aspect the device is connected between the second network and the computer system via the third and fourth communication interfaces. The device may enable or disable access to and from the second network, to the computer system, according to a selected mode of operation.

According to another aspect of the invention, the device provides an indication of the current mode of operation as well as indication relating to various situations such as alert, halt and the like. Respectively, the device may include a display unit, an audio generating unit, a vibration generating unit and the like. Alternatively, the device may utilize the multi-media capabilities of the computer station to produce these indications.

The device may further include a first reset input-output interface, connected to the managing controller, for connecting to an operating system source unit and a second reset input-output interface, connected to the managing controller for connecting to the computer system. The managing controller is operative to enable or deny the computer system access to the operating system source unit.

The operating system source unit is selected from the group consisting of a magnetic media drive, an optical media drive, an electro-optical media drive, a communication link and a non-volatile memory. It will be noted that non-volatile memory is selected from the group consisting of ROM, FLASH, EPROM, EEPROM, battery supported RAM and the like.

In accordance with a further aspect of the invention, there is provided a method for operating a communication controlling device. The device is connected between at least one storage unit, at least one peripheral device and a computer station. The device is operable to provide a first predetermined mode of operation and at least an additional different mode of operation.

3

The method includes the steps of:

detecting a boot signal received from the computer station;

executing a menu procedure;

receiving an instruction from a user to operate according to a selected mode of operation;

enabling access of the computer station to selected areas of the at least one storage unit according to the selected mode of operation; and

disabling access of the computer station to non-selected areas of the at least one storage unit according to the selected mode of operation;

enabling access of the computer station to selected areas of the at least one peripheral device, according to the selected mode of operation; and

disabling access of the computer station to non-selected areas of the at least one peripheral device, according to the selected mode of operation.

The method of the invention may also include the steps of:

receiving an instruction from a user to operate according to another selected mode of operation;

providing a restart command to the computer station;

detecting a boot signal received from the computer station;

enabling access of the computer station to selected areas of the at least one storage unit according to the other selected mode of operation; and

disabling access of the computer station to non-selected areas of the at least one storage unit according to the other selected mode of operation;

enabling access of the computer station to selected areas of the at least one peripheral device, according to the other selected mode of operation; and

disabling access of the computer station to non-selected areas of the at least one peripheral device, according to the other selected mode of operation.

The method of the invention may further include the steps of:

receiving an instruction from a user to operate according to another selected mode of operation;

providing a restart command to the computer station;

detecting a boot signal received from the computer station;

providing a boot command to the computer station;

enabling access of the computer station to selected areas of the at least one storage unit according to the other selected mode of operation; and

disabling access of the computer station to non-selected areas of the at least one storage unit according to the other selected mode of operation;

enabling access of the computer station to selected areas of the at least one peripheral device, according to the other selected mode of operation; and

disabling access of the computer station to non-selected areas of the at least one peripheral device, according to the other selected mode of operation.

The boot command may be a hardware boot command or a software boot command. The boot command may be followed by resetting the memory of the computer station.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the drawings in which:

4

FIG. 1 is a schematic illustration of a network providing secured information communication, constructed and operative in accordance with a preferred embodiment of the invention;

FIG. 2 is a schematic illustration in detail of the server of FIG. 1 and the communication controller, according to the invention;

FIG. 3 is a schematic illustration in detail of a node, shown in FIG. 1 and a communication controller therefor, according to the invention;

FIG. 4 is a schematic illustration in detail of another node shown in FIG. 1;

FIG. 5 is a schematic diagram of a method for operating a communication controller so as to provide limited communication access to a computer, operative in accordance with another preferred embodiment of the invention;

FIG. 6 which is a schematic illustration of a computer system and a device for securing the computer system during communication, constructed and operative in accordance with a further preferred embodiment of the invention;

FIG. 7 is a schematic illustration of a computer system and a device for securing the computer system and its environment during communication, constructed and operative in accordance with yet a further preferred embodiment of the invention;

FIG. 8 is a schematic illustration of a method for operating communication controllers shown in FIGS. 1, 6 and 7, operative in accordance with a further preferred embodiment of the invention;

FIG. 9 is a schematic illustration in detail of a further node, shown in FIG. 1;

FIG. 10 is a schematic illustration of a computer station and a communication device, constructed and operative in accordance with a preferred embodiment of the invention;

FIG. 11 is a schematic illustration of a computer system, a storage unit, a communication device and a portable unit, for securing the computer system during communication, constructed and operative in accordance with yet another preferred embodiment of the invention;

FIG. 12 is a schematic illustration of a log unit, constructed and operative in accordance with yet another preferred embodiment of the invention;

FIG. 13 is a schematic illustration of a method for operating the log unit of FIG. 12, operative in accordance with yet a further preferred embodiment of the invention;

FIG. 14 is a schematic illustration of a computer and a device, constructed and operative in accordance with a further preferred embodiment of the invention; and

FIG. 15 is a schematic diagram of a method for operating an I/O and communication controlling device so as to provide limited data and communication access to a computer, operative in accordance with another preferred embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention includes several aspects which define novel principles for transmitting and storing data in a multiple computer system.

According to one aspect of the invention, secured areas and public areas are physically separated. Thus, a network system according to the invention shall include at least two communication networks wherein at least one of these networks is defined as a secured network, whereby confi-

5

dential information is generally transmitted via the secured area. There is no direct connection between the public network and the secured network.

According to another aspect of the invention, confidential transmissions are physically divided into at least two elements wherein at least a predetermined one of them is required to reconstruct the original transmission. This predetermined element is transmitted via a secured network and stored in a secured storage area, both of which can be physically disconnected from a main channel of communication.

According to a first implementation of the invention, the first element includes a portion of the classified data and the second element includes a complementary element of the classified data.

According to a second implementation of the invention, the first element includes the classified data in an encrypted form and the second element includes the encryption-decryption software.

According to a third implementation of the invention, the first element includes the classified data in an encrypted form and the second element includes the encryption-decryption key.

Reference is now made to FIG. 1 which is a schematic illustration of a network providing secured information communication, generally referenced 1, constructed and operative in accordance with a preferred embodiment of the invention.

Network 1 includes a plurality of nodes, referenced 20, 30, 40, 50, 60 and 70, a server 4, a public network 6 and a secured network 8. All of the nodes 20, 30, 40, 50, 60 and 70 are interconnected via public network 6.

According to the present example, nodes 20, 30, and 40 are also interconnected via secured network 8. The public network 6 is also connected to an external network which in the present example is the Internet 80.

Server 4 includes a Central Processing Unit 10 (CPU), a storage unit 14 and a controller 12. The controller 12 is adapted to receive transmissions from networks 6 and 8 and write them in various locations in the storage unit 14. The storage unit is divided into at least two areas, a public area 16 and a secured area 18. The public area 16 contains non-confidential information whereas the secured area 18 contains classified information.

Node 20 is a secured node which is able to transmit and receive confidential information over the networks 6 and 8. The node 20 includes a computer station 21, a storage unit 22 and a communication controller 28. Communication controller 28 is connected to the computer station 21, the storage unit 22, the public network 6 and the secured network 8. The storage unit 22 is divided into two storage areas, a public storage area 26 and a secured storage area 24.

The communication controller 28 controls all communication to and from node 20. The communication controller 28 provides access to the public storage area 26 to both networks 6 and 8. The communication controller 28 provides, only the secured network 8 with access to the secures storage area 24.

At node 20, all of the communication with the public network 6 goes through the communication controller 28. Thus, the communication controller 28 monitors and controls all communications between the computer 21 and the public network 6.

Node 30 is a secured node which is able to transmit and receive confidential information over the networks. The

6

node 30 includes a computer station 31, a storage unit 32 and a communication controller 38. Communication controller 38 is connected to the computer station 31, the storage unit 32, the public network 6 and the secured network 8. The computer 31 is also connected to the public network 6. The storage unit 32 is divided into two storage areas, a public storage area 36 and a secured storage area 34.

The communication controller 38 monitors all of the communication transmissions received from the public network so as to detect access attempts to the secured storage area 34. When such an attempt is detected, the communication controller denies access to the secured area 34 and executes an alert procedure to alert the user of the node 30.

Node 40 is a secured node which is able to transmit and receive confidential information over the networks 6 and 8. The node 40 includes a computer station 41, a public storage unit 46, a secured storage unit 44 and a communication controller 48. Communication controller 48 is connected to the computer station 411 the secured storage unit 44, and the secured network 8. The computer 41 is also connected to the public network 6 and to the public storage unit 46.

The communication controller 48 provides access to the secured storage unit 44. The public network 6 has access to the public storage area 46 via the computer 41.

Node 50 is a non-secured node having a storage unit 54 and a computer 52, connected thereto and to the public network 6. Node 60 is a non-secured node having a storage unit 64 and a computer 62. Both the storage unit 64 and a computer 62 are interconnected as well as connected to the pubic network 6.

It will be noted that nodes 50 and 60 are connected to the public network 6 only and thus are not authorized to access any confidential information which is stored on any of the secured storage areas 18, 24 34 and 44.

Node 70 is a locally secured node having a computer 71, a storage unit 72 and communication controller 78. The storage unit 72 is divided into two storage areas, a public storage area 76 and a secured storage area 74.

The communication controller 78 is connected to the storage unit 72, the public network 6 and to the computer 71. The computer 71 is connected to the public network 6. When the communication controller 78 detects that the computer 71 is in communication with the network 6, it denies any access to the secured storage area 74.

According to the invention, each of the communication controllers 12, 28, 38, 48 and 78 monitors all of the communication transmissions received from the public network 6 so as to detect access attempts to a respective secured storage area connected thereto. When such an attempt is detected, the respective communication controller denies access to the relevant secured area and executes an alert procedure to alert any user using the node or server.

According to the present invention, all of the above three implementations for determining the first and second segments are available for the present example, wherein the first segment is stored in a public storage area of the receiving node and the second segment is stored in a secured storage area of the receiving node. It is noted that for such matters, a server can be considered a node.

According to the invention, non-confidential data from any node to any node can be transmitted over the public network 6 and stored in a public storage area of the receiving node. Confidential information can be transmitted over the public network 6, divided into a first and second segments and stored accordingly wherein the first segment is stored in

the public storage area of the receiving node and the second segment is stored in the secured storage area of the receiving node.

For example, retrieving confidential information from the server 4 is performed by transmitting a retrieval request divided into two segments where the first segment is transmitted over the main network 6 and to the destination node and the second segment is transmitted to the destination node over the secured network 8. Hence, only nodes which are connected to the secured network 8 receive the two segments which are required to reconstruct the classified information.

Thus, a request for altering data stored in the secured area 18 will only be performed if received, at least partially, via the secured network 8.

Dividing a file into segments can be performed according to numerous ways such as generating the first segment from all of the odd bits in the original file and generating the second segment from all even bits in that original file, splitting the file in half, splitting the file into a predetermined large number of segments, and the like.

According to one aspect of the invention, the public network 6 and the secured network 8 are both implemented on the same communication medium, in different ways. For example, the public network 6 is represented by a modulated transmission in a first predetermined frequency and the secured network 8 is represented by a modulated transmission in a second predetermined frequency. Furthermore, any of communication networks 6 and 8 may consist of cable communication, wireless communication, optical communication and the like.

According to the present example, communication of confidential information between two nodes can be performed only between nodes which are connected via the secured network 8. For example, when node 40 needs to transfer confidential information to node 20, the confidential information is divided into two elements. The two elements are transmitted from node 40 to node 20 wherein the first element is transmitted over the public network 6 and the second element is transmitted over the secured network 8.

Reference is now made to FIG. 2 which is a schematic illustration in detail of server 4 of FIG. 1 and the communication controller 12 according to the invention.

The communication controller 12 includes a network interface 92, connected to the public network 6, a network interface 90 connected to the secured network 8, an input-loutput (I/O) interface 96 connected to the storage unit 14, an I/O interface 94 connected to the CPU 10 and a managing controller 98. The managing controller 98 is also connected to the network interface 92, the network interface 90, the I/O interface 96 and the I/O interface 94.

The managing controller 98 provides access to the secured storage area 18 only to access requests which are provided via the secured network 8.

According to the invention, an access request may include several data segments wherein some of these segments are received from the public network 6 and the rest are received from the secured network 8.

The managing controller 98 combines these data segments back to form the original access request and executes it.

Thus, information can be stored in the secured storage area 18 in two cases, either if at least partially received from the secured network 8 or if originally determined as confidential information by one of the computers 20, 30 and 40,

connected to the secured network 8. It will be appreciated that security is enhanced when all of the secured information is transmitted over the secured network 8.

According to the invention, a confidential information file arrives at the server 4 divided into at least two segments. This confidential information file can be stored either in the secured storage area 18 or both in the secured storage area 18 and the public information storage area 16, according to several storing and retrieving modes.

According to one storing mode, the managing controller 98 receives the confidential information file divided into several segments. The managing controller 98 then stores some of these segments in the secured storage area 18 and the rest of the segments in the public storage area 16.

According to another storing mode, the managing controller 98 combines all of the segments to form a single file and stores it in the secured information storage area 18.

According to a further storing mode, the managing controller 98 stores the confidential information file in the secured storage area in a segmented form. According to this mode, when requested to retrieve this information from the storage unit 14, the managing controller 98 accesses the segments which form the confidential information file and transmits them without any processing, reassembling and the like.

According to another aspect of the invention, the server 4 reassembles the original file of the confidential information from segments of the classified information and stores it as one file in the secured information storage area 18.

Reference is now made to FIG. 3 which is a schematic illustration in detail of node 20 of FIG. 1 and the communication controller 28 according to the invention.

The communication controller includes a communication interface 150 for connecting to the public network 6, a communication interface 154 for connecting to the secured network 8 and a switching unit 152 for directing data inside the node 20. Communication of node 20 to any of the two networks 6 and 8 must be performed via the communication controller 28.

Reference is now made to FIG. 4 which is a schematic illustration in detail of node 30 of FIG. 1.

The computer 31 includes a working station 33 and a communication interface 35, connected thereto. The communication controller 38 includes a communication detector 162, a managing controller 160, a computer interface 166, an I/O interface 164 and a communication interface 168.

The communication detector 162 is connected to the managing controller 160 and to the public network 6 for detecting communications received by computer 31. The computer interface 166 is connected to the managing controller 160 and to the computer 31. The I/O interface is connected to the managing controller 160 and to the storage unit 32.

The communication interface 168 is connected to the managing controller 160 and to the secured network 8.

Communication interface 168 is a conventional WAN or LAN interface, such as a modem or an Ethernet interface. According to the present example, the computer 31 can communicate over the public network 6 directly via the communication interface 35.

The computer 31 receives access requests from public network 6 via the communication interface 35. The computer 35 provides these requests to the managing controller 160 via the computer interface 166.

The managing controller 160 retrieves the information from the public storage unit 36 and provides it to the

computer 31 which, in turn, transmits it to the public network 6 via the communication interface 35.

The managing controller 160 also detects access requests directly from the public network 6 and processes them. If the managing controller 160 detects an information request which relates to information stored in the secured storage area 34, a corresponding request for this information provided by the computer 31 will be denied.

It is noted that non-restricted communication between the public network 6 and the non-secured areas of node 30, such as the computer 31 and the public storage area 36, is provided directly via the communication interface 35 and as such is not interrupted by the communication controller 38.

The communication controller 38 also provides a full separation security mode. According to this mode, when the communication detector 162 detects that the computer 31 is communicating with the public network 6, it physically disables the I/O interface 164 and the communication interface 168, thus eliminating any access to the secured storage area 34 and to the secured network 8.

Referring back to FIG. 1, there is provided a further aspect of the present invention, in which node 40 is defined as a security supervising station. Thus, when a secured node such as node 20 wants to transmit data from the secured storage area 24 to a non-secured node, for example to node 50, node 20 transmits this data to node 40. Node 40, receiving this data, stores it in the secured storage unit 44 and also provides it to the supervisor. When the supervisor provides his authorization, the node 40 transferes the data to public storage unit 46 and further transmits it to node 50. According to an additional aspect of the invention, node 40 operates as a "Store-and-Forward" buffer whereby at any point in time, it is either in communication with the public network 6 or with the secured network 8, but not to both networks. This means that the communication controller 48 provides communication with the secured network 8 only when the computer 41, disconnects from the public network 6. According to this aspect of the invention, there can be no on-line communication between the public network 6 and secured network 8, via node 40.

Reference in now made to FIG. 5 which is a schematic diagram of a method for operating a communication controller so as to provide limited communication access to a computer, operative in accordance with another preferred embodiment of the invention.

In step 200, the communication controller receives a transmission.

In step 202, the communication controller determines the type of request contained in the received transmission. If the received transmission contains a write access request, such as alter data, format, delete, move, copy and the like, then the controller proceeds to step 204. If the received transmission contains a read access request, then the controller proceeds to step 220.

In step 204, the communication controller determines if at least a portion of the transmission was received via the secured network. If so, then the communication controller proceeds to step 206. Otherwise, the communication controller proceeds to step 214.

In step 206, the communication controller determines a storing mode, as described hereinabove, according to which the transmission will be stored and proceeds to a respective step 208, 210 and 212.

In step 214, the communication controller determines if the requested destination of the transmission is the secured

area. If so, then the communication controller proceeds to step 218. Otherwise, the communication controller proceeds to step 216.

In step 216, the communication controller stores the transmission in the public storage area.

In step 218, the communication controller executes an alert procedure. Such an alert procedure can be denying access to the secured area, producing an alert message or signal to the user operating the computer connected to the communication controller, halting selected activities in the node including the communication controller, and the like.

For reading, the communication controller determines (in step 220) if at least a portion of the transmission was received via the secured network. If so, then the communication controller proceeds to step 222. Otherwise, the communication controller proceeds to step 224.

In step 222, the communication controller retrieves data, according to the access request contained in the transmission.

In step 224, the communication controller determines if the requested destination of the transmission is the secured area. If so, then the communication controller proceeds to step 218. Otherwise, the communication controller proceeds to step 226.

In step 226, the communication controller retrieves data, from the public storage area, according to the access request contained in the transmission.

Reference is now made to FIG. 6 which is a schematic illustration of a computer system, referenced 390, and a device, referenced 300, for securing the computer system during communication, constructed and operative in accordance with a further preferred embodiment of the invention.

Computer system 390 includes a Central Processing Unit (CPU) 310, a memory unit 314, a storage unit 316, a communication interface 312 for connecting to a communication network 324 and a communication bus 322. The device 300 according to the invention includes a processor 302 and a switching unit 304 connected thereto.

The storage unit 316 is divided into two areas, a public area 318 and a secured area 320. The device 300 controls the storage unit 316 so as to provide full access to the public area 318 via communication bus 322, to all of the components of the computer system 390 such as the CPU 310 and the communication interface 312.

The processor 302 controls the switch 304 so as to allow or deny access to the secured area 320. According to one aspect of the invention, the device 300 provides analysis management during and right after communication. Denying access to the secured area 320 can be implemented in several manners which include denying full access, providing read only access and the like.

According to the invention, during on-line communication with the network 324, the device 300 disconnects the secured area 320 from the computer system and denies all access to it. In addition, the processor 302 monitors all data transfer on communication bus 322, detects data changes in the public area 318 of storage unit 316 and generates a log file therefrom.

When the computer system 390 is disconnected from the network 324, the processor 302 retrieves an analysis software application from the secured area, generates a security key and provides the security key to the analysis software. In the present example, the analysis software application is an anti-virus scanning software. Then, the processor 302 provides the analysis software application to the CPU 310.

11

12

The CPU 310 executes the analysis software application according to the log file on all of the data changes in the public area 318.

If the analysis software application does not detect any hostile software or in that matter, any suspicious data change, it returns the security key to the processor 302. Then, the processor 302 operates switching unit 304 so as to enable access to the secured area 320.

The device 300 is operative to deny access to the secured area 320 according to several method and parameters. According to one aspect of the invention, the secured area 320 is defined physically according to address. Thus, access is denied to selected addresses and provided to all the rest. A processor for this implementation may consist of a few logical NAND gates which automatically deny access to the secured area addresses.

According to another aspect of the invention, the secured area 320 is defined according to logical address, such as file name, directory name, logical attributes, and the like, to which access is denied.

Detection of an on-line communication situation is possible in several methods. According to one method, detection is provided via a direct connection to the communication line via a dedicated communication interface, as described in conjunction with communication controller 28 of FIG. 3, thus monitoring all activity therein. Alternatively, the device 300 is indirectly connected to the communication line, for example, by sensing the electromagnetic field produced in the vicinity of the communication cable, as indicated by reference 328, thus monitoring all activity therein. Further, either the computer system 390 or the communication interface provide information relating to the communication status to the device 300. Still further, a designated software application, such as a communication software provides information relating to the communication status to the device 300.

Reference is now made to FIG. 7 which is a schematic illustration of a computer system, referenced 490 and a device, referenced 400, for securing the computer system and its environment during communication, constructed and operative in accordance with yet a further preferred embodiment of the invention.

Computer system 490 includes a Central processing unit (CPU) 406, a memory unit 410, a storage unit 416, a WAN communication interface 408 for connecting to a WAN communication network 428, a LAN communication interface 424 for connecting to a LAN communication network 426 and a communication bus 422. The device 400 includes a processor 402 and a switching unit 404 connected thereto. It will be appreciated that this is a non-limiting example and that each of communication networks 428 and 424 can be any type of network such as a WAN, a LAN, a wireless communication network, an optical based network and the like.

The storage unit 416 is divided into two areas, a public storage area 418 and a secured storage area 420. The memory unit 410 is divided into two areas, a public memory area 412 and a secured memory area 414. According to one aspect of the invention, the two storage areas 418 and 420 can be a single storage unit which is divided into two parts, which is fully controlled by the device 400.

According to another aspect of the invention, the two storage lo areas 418 and 420 are two separate storage units which are not interconnected, whereas the device 400 fully controls the access to the secured storage area 418 and is adapted to perform an analysis procedure on the public storage area 420.

According to a further aspect of the invention, each of the storage areas 418 and 420 includes several storage units.

The public storage area 418, the public memory area 412, the CPU 406, the WAN communication interface 408 and the device 400 are interconnected via the communication bus 422.

The secured storage area 420, the secured memory area 414 and the LAN communication interface 424 are connected to the switching unit 404.

The processor 402 controls the switching unit 404 so as to allow or deny access to the secured storage area 420, the secured memory area 414 and the LAN communication interface 424. Access is denied when the computer system 490 is in communication with the WAN network via the WAN communication interface 408.

The device 400 operates generally similar to device 300. The device 400 is thus operative according to the method described hereinbelow with respect to FIG. 9 whereas, as long as a security flag, determined in this method, is on, access is denied to the secured storage area 420, the secured memory area 414 and the LAN communication interface 424.

According to a further aspect of the invention, the processor 402 is operative to execute an analysis software application in the secured memory area 414, which scans the public memory area 412 and the public storage area 418 after WAN communication is disconnected. Thus, the analysis software application is never accessible to unauthorized elements such as hostile programs or outside users.

According to the present invention, the device 400 can deny access to any device connected thereto, during communication, so as to prevent unauthorized access.

Reference is now made to FIG. 8 which is a schematic illustration of a method for operating devices 28, 38, 48 (FIG. 1), 300 (FIG. 6) and 400 (FIG. 7), operative in accordance with a further preferred embodiment of the invention. In the present example, the description refers to device 300 and computer system 390 of FIG. 6. The method includes the following steps:

In step 500, the device sets a security flag to off.

In step 502, the device 300 detects if the computer 390 performs on-line communication. If so, the device proceeds to step 504. Otherwise, the device proceeds to step 507. Off-line communication is defined either when the communication interface (for example, the modem) is disconnected from the network, or when the computer is disconnected from the communication interface, either temporarily, or permanently, while communication interface stays connected and communicating with the network.

In step 504, the device 300 disconnects the secured area 318 from the rest of the computer system 390.

In step 506, the device 300 turns the security flag on and generates a log file of the data changes which occur in the computer system 390 and its public storage area, during communication, due to incoming data and the like. At the same time, the device proceeds back to step 502 for confirming that communication is on-line.

In step 507, if the security flag is on, then the device proceeds to step 508. Otherwise the device proceeds back to step 502.

In step 508, the device 300 generates a security key and proceeds to step 510.

In step 510, the device 300 retrieves an analysis software application from the secured area, provides the security key to the analysis software application and provides them both to the CPU 310.

In step **512**, the CPU executes the analysis software application, on all data changes which, according to the log file, occurred during on-line communication. The analysis software application detects if any hostile attempt was made to damage the information contained therein. If so, the computer system **390** proceeds to step **516**. Otherwise, the system **390** proceeds to step **514**.

In step **514**, the analysis software application returns the security key to the processor **302**, which in turn enables access to the secured area **320** and proceeds back to step **500**.

In step **516**, the computer system **390** provides the user with a warning and halts.

The security key is preferably generated according to a momentary data situation in the secured area **320**. The security key can also be generated as a one time key which is independent of the secured area **320**, such as according to an internal random generator and the like. The main reason for this is to minimize and preferably eliminate all possible access to this security key from elements which are not authorized and which may attempt to try to provide this key to the processor **302**.

Reference is now made to FIG. **9** which is a schematic illustration in detail of node **70** of FIG. **1**.

The communication controller **78** according to the invention includes a processor **602**, a switching unit **604**, a communication interface **606**, an input-output (I/O) interface **608**, a computer interface **610**. Communication controller **78** is connected to a network **6** via the communication interface **606**, to storage unit **72** via I/O interface **608** and to the computer system **71** via computer interface **610**. The storage unit **72** is divided into two major sections, a public section **76** and a secured section **74**. According to the present example, I/O interface is either an IDE-ATA or SCSI disk controller.

The communication interface **606** is selected according to the type of network **6** and is selected from the group consisting of a dial-up modem, a WAN modem, a LAN modem, an optical modem, an ISDN modem, a cable television modem, and the like. The communication interface **606** may also be an I/O interface for connecting to a modem of any kind. The processor **602** controls the on-line physical connection of the computer station, the storage unit **72** and the network **6**, therebetween.

The communication controller **78** is operative according to several modes of operation. According to one mode of operation, the communication controller **78**, when receiving a communication request command from the computer system **71**, operates the communication interface **606**, so as to provide communication with network **6**. At the same time, the communication controller **78** monitors all access requests to the storage unit **72**, allows access to the public area **76** and denies access to the secured area.

According to a second mode of operation, when the computer system **71** provides the communication controller with a request to access the secured area **74**, the communication controller **78** operates the switching unit **604** so as to disconnect the computer from the communication interface **606**, while maintaining communication between the communication interface **606** and the network **6**.

At that point, the processor **602** scans the public area **76** as well as any other storage unit in computer system **71** so as to detect harmful programs which may cause damage to the secured area. If such programs are not detected, the communication controller provides the computer system **71** with access to the secured area **74**. When the computer system provides the communication controller **78** with a command to reconnect to the network, the communication controller **78** reconnects the computer system **71** with the communication interface **606** and simultaneously denies all access to the secured area **74**.

According to a third mode of operation, the communication controller **78** terminates the communication with network **6** and the processor **602** scans the public area **76** as well as any other storage unit in computer system **71** so as to detect harmful programs which may cause damage to the secured area. If such programs are not detected, the communication controller provides the computer system **71** with access to the secured area **74**.

It will be appreciated that the processor **602** can either scan or execute a scanning and analyzing software which is designed for this purpose. According to the present invention, the method described in FIG. **8**, can be implemented in communication device **78**.

It is noted that the processor **602**, by controlling switching element **604** and communication interface **606**, can disconnect the computer **71** from the network either by providing communication interface **606** with a command to terminate communication with network **6** or by operating switching element **604** so as to disconnect communication interface **606** from the computer **71** while maintaining the connection between the communication interface **606** and the network **6**.

According to the invention, the processor **602** is also operative to receive, from the computer **71**, commands to disconnect communication between the communication interface **606** and the network **6** or between the communication interface **606** and the switching element **604**.

Reference is now made to FIG. **10** which is a schematic illustration of a computer station and a communication device, generally references **650**, constructed and operative in accordance with a preferred embodiment of the invention.

Device **650** includes a communication interface **656**, a storage unit **654** and a switching unit **662**. Communication interface **656** is connected to switching unit **662** and to a communication line **658**, which is further connected to a communication network **660**. Device **650** is connected to a data bus **664** of a computer **652** which further includes a processor **666** and a storage unit **670**.

Communication interface **656** can be a conventional modem, a modem emulator, a network communication card, and the like. Storage unit **654** can be any type of data storage device such as ROM, RAM, flash memory, a disk, tape and the like. Some implementations of the invention such as the first one, require dynamic readnwrite storage units such as RAM, flash memory, a disk and the like, since the data stored in the secured storage unit is dynamic. Other implementations such as the second and third ones can use less dynamic storage units such as ROM, EPROM, EEPROM and the like, which are likely to simplify the overall structure and reduce the cost of manufacturing the device **650**.

The device **650** is operative according to several modes, which enhance the security of confidential information against unauthorized access attempts from the network **660**. Disclosed hereinafter are a number of non-restricting, exemplary modes.

According to a first mode, any confidential data file which needs to be secured is divided into two segments. The first segment is stored in the storage unit **670** of computer **652** and the second segment is stored in storage unit **654** of device **650**. The division is performed so that reconstructing the original file using the first segment alone is likely to be extremely difficult which, in practice, may be considered impossible.

According to another mode, confidential data contained in storage unit 670 is encrypted using an exclusive encryption key, wherein is when the encryption is complete, the key is stored in storage unit 654.

According to a further mode, all of the confidential data is stored in storage unit 654.

The computer 652 is able to communicate with the network via the communication interface 656, as indicated by the dotted line 668. When the computer 652 does not communicate with the network 660, the switching unit 662 disconnects the bus 664 from the communication interface 656 and connects the storage unit 654 to the bus 664, as indicated by line 672.

When the computer establishes a communication connection via communication interface 656, switching unit 662 disconnects storage unit 654 from the bus 664 and connects the communication interface 656 to the bus 664. Thus, any party communicating with the computer 652 has limited data access which is confined to the data stored in the computer storage unit 670 and not to the data contained in storage unit 654.

It will be appreciated that when the switching unit 662 disconnects the storage unit 654 from the bus 664 it makes the storage unit and all of the data contained therein unavailable.

The communication device 650 can be implemented as an add-on internal card according to conventional standards such as an AISA, VLB, PCI, PCMCIA and the like. The device can also be implemented as an external device for connecting via a serial port, a parallel port and the like. Thus, for example, the device 650 can be implemented as PCM-CIA modem card for a portable computer. The user can remove the communication device from the computer 652 and use it as a key. It will be appreciated that as long as the communication device 650 is not connected to the computer 652, there is no access to any data contained inside storage unit 654.

According to the present invention, the method described in FIG. 8 can be implemented in communication device 650.

Reference is now made to FIG. 11 which is a schematic illustration of a computer system, referenced 890, a storage unit, referenced 810 a device, referenced 800 and a portable unit 850, for securing the computer system during communication, constructed and operative in accordance with yet another preferred embodiment of the invention.

The computer system 890 is connected to a communication network 892 and to the device of the invention 800. The device 800 is also connected to storage unit 810. The device 800 includes a processor 802, a switching unit 804 and a wireless transceiver 803.

The portable unit 850 includes a wireless transceiver 852 and a processor 854, connected thereto.

The storage unit 810 is divided into five areas:

a log area 812, for managing a log file;

a buffer area 814, for intermediately storing data upon receipt but before it is transferred into a secured area 820;

a public area 816, which is accessible at all times;

a read only area 818, for storing operating unit files, analysis software application and the like; and

a secured area 820 for storing confidential information.

The device 800 manages the storage unit 810 as follows. When the computer system 890 is in an on-line communication with the communication network 892, the device 800 enables full access to the public area 816 and to the buffer

area 814, for reading and writing. The device 800 also enables limited read-only access to the read only area 818. Simultaneously, the device 800 updates the log area with information relating to data changes in the storage unit 810 and data requests received from the computer system 890. The device 800 denies access to the secured area 820. After the computer system 890 is disconnected from the communication network 892, the device 800 retrieves an analysis software application from the read only unit and executes it, according to the information contained in the log area 812, on the data contained in the public area 816 and the buffer area 814. Any data which is destined for the secured area 820 is transferred from the public area 816 to the buffering area 814, scanned and, if classified as harmless, transferred to the secured area 820.

According to the present embodiment, the device 800 is operable to provide access secured areas in the storage unit 810 only when an authorized user, wearing the portable unit 850, is in the vicinity of the device 800.

According to a wireless mode of the invention, the wireless transceiver 852 transmits a signal to the wireless transceiver 803. The wireless transceiver 803 detects this signal and provides it to the processor 802 which regards it as an enable signal to provide access to the secured areas in storage unit 810. According to this mode, if the user has left the premises and wireless transceiver 803 does not detect the signal transmitted by the wireless transceiver 852, the device 800 denies access to the secured areas of the storage unit 810.

According to another wireless mode, the processor 854 provides the wireless transceiver 852 commands to transmit a different signal from time to time. The processor 802 is then adapted to recognize the various signals or the change between them.

According to a further wireless mode, wireless transceiver 803 and wireless transceiver 852 communicate using bidirectional communication. Thus, the processors 802 and 854 are operative to exchange decoded signals, so as to enhance even more the level of security.

Reference is now made to FIG. 12 which is a schematic illustration of a log unit, referenced 1000, constructed and operative in accordance with yet another preferred embodiment of the invention.

The log unit 1000 includes a storage area 1002 and a controller 1004 connected thereto. The controller 1004 is operative to provide sequential writing of log entries in the storage unit as well as random-access reading of log entries contained therein.

According to the invention, when the controller 1004 receives a write-command to register a new log entry, it ignores the address which may be incorporated in the write-command and assign an address which is in sequence with the address of the previous write-command. Thus, an attempt to change a preselected log entry with a write-command which includes a specific address will not be executed. According to one aspect of the invention, when such an attempt occurs, the controller 1004 produces an alert command to a computer (not shown) connected thereto.

One of the main advantages of this log unit is that it does not permit free writing access to the log area, thus preventing any deliberate change of a preselected log entry.

When a log file is located in a finite size storage area, sometimes it exceeds the limit of storage space. The common solution in this situation is to define the log file as a cyclic file, i.e. after writing the last possible entry, at the end of the log file, then start writing at the beginning of the log

file. Thus, if one wishes to change the log file, he may write as many log entries needed to fill and rewrite the entire log file.

The method according to the invention, overcomes this problem by providing a minimum time period between two sequential log entry write commands. Thus, writing over an entire log file is limited so that one cannot be performed it in a short period of time.

Reference is now made to FIG. 13 which is a schematic illustration of a method for operating the log unit 1000 of FIG. 12, operative in accordance with yet a further preferred embodiment of the invention.

In step 1050, the log unit 1000 receives a log command.

In step 1052, if the received log command is a write command, then the log unit 1000 proceeds to step 1056. Otherwise, if the received log command is a read command the log unit 1000 proceed to step 1054.

In step 1054, the log unit 1000 retrieves a requested log entry.

In step 1056, if the time period Δ is greater than or equal to a predetermined period of time T, then the controller 1004 proceed to step 1060. Otherwise, the controller 1004 proceeds to step 1058.

In step 1058, the controller 1004 denies access to the to the storage area 1002.

In step 1060, the controller 1004, retrieves the log information from the log command and proceeds to step 1062.

In step 1062, the controller 1004 provides a log address which is in sequence with the address of the previous write-command.

In step 1064, the controller 1004 writes a log entry containing the log information at the log address.

According to a further aspect of the invention, step 1058 may also include producing an alarm signal to alert a supervisor, and the like.

Reference is now made to FIG. 14 which is a schematic illustration of a computer 1102 and a device, generally referenced 1100, constructed and operative in accordance with a preferred embodiment of the invention.

The device 1100 includes a managing controller 1122, two disk drive input-output (I/O) interfaces 1118 and 1120, an I/O switching unit 1139, two diskette drive input-output (I/O) interfaces 1137 and 1138, a first pair of communication interfaces 1110 and 1112 for connecting the computer 1102 to a public network 1136 and a pair of communication interfaces 1114 and 1116 for connecting the computer 1102 to a secured network 1134, two communication switches 1140 and 1142 and a display 1144, connected to managing controller 1122.

Disk drive input-output (I/O) interfaces 1118 and 1120 are connected to managing controller 1122. I/O switching unit 1139 is connected to the two diskette drive input-output (I/O) interfaces 1137 and 1138 and to managing controller 1122.

Communication interface 1110 is connected to communication switch 1142 and to the computer 1102. Communication interface 1112 is connected to communication switch 1142 and to the public network 1136. Communication switch 1142 is connected to managing controller 1122.

Communication interface 1114 is connected to the communication switch 1140 and to the computer 1102. Communication interface 1116 is connected to the communication switch 1140 and to the secured network 1134. The device 1100 is connected to a storage unit 1124 via I/O

interface 1120. The storage unit 1124 is divided into a plurality of areas: a menu area 1126, a secured area 1130, a public area 1128, a log area 1132 and a password area 1133.

The public area 1128 contains data and software which are not confidential. The secured area 1130 contains data and software which are confidential. The log area 1132 contains a log file architecture according to conventional methods or according to the invention, as described hereinabove. The password area 1133 contains passwords which may be utilized during various procedures by the managing controller 1122, such as switching between modes and the like.

The menu area 1126 includes a pre-operation system menu, which manages the computer 1102 as the computer 1102 is booted up (i.e., started or restarted). This menu is loaded into the computer 1102, and the user is requested to choose between working modes, a public mode and a secured mode.

If the user chooses to work in the secured mode, then the computer provides this selection to the managing controller 1122 which, in turn, performs the following actions:

connects the secured area 1130 to the computer 1102;

denies access to the public area 1128;

provides communication switch 1140 with a command to enable connection between communication interfaces 1114 and 1116, thus connecting the computer 1102 and the secured network 1134; and

provides communication switch 1140 with a command to deny any connection between communication interfaces 1110 communication and 1112, thus disconnecting the computer 1102 from the public network 1136.

If the user chooses to work in the public mode, then the computer provides this selection to the managing controller 1122 which, in turn, performs the following actions:

connects the public area 1128 to the computer 1102;

denies access to the secured area 1130;

provides communication switch 1142 with a command to enable connection between communication interfaces 1110 and 1112, thus connecting the computer 1102 and the public network 1136; and

provides communication switch 1142 with a command to deny any connection between communication interfaces 1114 communication and 1116, thus disconnecting the computer 1102 from the secured network 1134.

According to the present invention, the device is operable on one of these two modes, the public mode and the secured mode. The public area 1128 and the secured area 1130 each includes an entire operating system. A change of mode is possible only through resetting the computer 1102 and loading an operating system from the selected area, according to the selected mode.

Conventional software, such as programs designed for IBM-PC architecture, do not make any use of disk addresses which begin with 0,0,# except 0,0,1, which contains the primary partition table.

According to a non-limiting example of the present invention, the addresses beginning with 0,0,1 include the partition table of the secured area 1130, the addresses beginning with 0,0,2 include the menu procedure, the addresses beginning with 0,0,3 include the partition table of the public area 1128, the addresses beginning with 0,0,4 include a pointer to the log area 1132 and the addresses beginning with 0,0,5 include the password area 1133.

According to the present example, the managing controller 1122 denies all write access to the addresses beginning with 0,0,2, which include the menu procedure. It will be

19
20

noted that, physically, the device controls all access to all addresses and is able to provide the computer 1102 with various access types such as read, write and the like of selected addresses.

This arrangement provides considerable protection to the areas of the storage unit, which are associated to addresses 0,0,2 and higher when the storage unit 1124 is connected directly to another computer which does not have a managing controller. It will be appreciated that this arrangement is most suitable for portable hard disk drives.

According to the present example, the device 1100 detects when the computer 1102 is reset and, at that point, provides access to the menu area 1126. When the device 1100 receives the mode selection from the computer, it resets the computer physically and connects it to either the public area 1128 or to the secured area 1130, according to the selected mode.

In conventional computer systems, the operating system can be loaded from several alternative sources which, for example, are the local hard disk drive, a diskette drive, the CD-ROM drive, a network connected to the computer and the like. According to the present invention, some of these sources are predetermined as unauthorized to provide an operating system and thus are disabled from doing so.

In the present example, the device 1100 can be adapted to secure the computer 1102 from accidental loading of an operating system which is received from an unauthorized source.

In the present example, the device 1100 controls the access to a diskette drive 1135 which otherwise would be connected directly to the computer 1102. When the computer requires loading of an operating system, the managing controller 1122 detects this request and accordingly provides I/O switching unit 1139 with a command to disconnect between diskette drive input-output (I/O) interfaces 1137 and 1138, thus denying access to diskette drive 1135.

After the computer 1102 commences loading an operating system from storage unit 1124, the managing controller 1122 provides I/O switching unit 1139 with a command to connect between diskette drive input-output (I/O) interfaces 1137 and 1138, thus enabling the computer 1102 to access the diskette drive 1135.

According to a further aspect of the present invention (not shown), in which the diskette drive 1135 is connected directly to the computer 1102, the managing controller 1122 measures the time period $T_{measured}$ between computer boot-up and loading of an operating system.

The access and data transfer rate provided by a hard disk drive are considerably faster than those provided by a diskette drive. Furthermore, initial access to a diskette drive, before an operating system was loaded, is considerably slower, compared with hard disk drives. Hence, $T_{measured}$ would be considerably greater when accessing a diskette drive compared with accessing a hard disk drive.

T_{boot} is a predetermined value which represents a predetermined maximal time period required to load an operating system from a hard disk drive. T_{boot} of a hard disk drive is shorter than that of a diskette drive. Thus, if $T_{measured} \geq T_{boot}$, then the managing controller 1122 detects that an unauthorized loading of an operating system is in progress and hence, may take several preventive measures, such as denying all access to storage unit 1124.

When the managing controller 1122 detects a diskette drive boot attempt, it may operate to halt all operations and provide an alarm, using the computer 1102 multi-media capabilities or an external alarm device and the like.

Furthermore, the managing controller 1122 can provide computer 1102 with a command which will disable opera-

tions therein, either fully or partially. For example, the managing controller 1122 can provide computer 1102 with a constant boot command.

Display 1144 indicates the current mode of the device. Display 1144 is adapted to be attached to the computer 1102 to be seen by the user. According to one aspect of the invention, display 1144 is a light emitting diode (LED) or a LED array which either blinks differently or changes color in various modes. According to the invention, display 1144 can also be a liquid crystal display (LCD) array, displaying alpha-numerical messages and the like.

It will be noted that, according to another aspect of the invention, the managing controller 1122 detects all data received from the diskette drive 1135, thereby enabling operating system loading access thereto in predetermined cases, such as maintenance. Operating system loading access to diskette drive 1135, may be provided to the computer 1102 only if a predetermined password is provided thereto while executing the menu procedure.

Reference is now made to FIG. 15 which is a schematic diagram of a method for operating device 1100 so as to provide limited data and communication access to a computer, operative in accordance with another preferred embodiment of the invention.

In step 1150, the managing controller 1122 detects a boot signal provided by the computer 1102. This signal is provided when the user manually boots up the computer or when the computer is turned on. According to the present example, the managing controller 1122 regards the first attempt to access address 0,0,1, via the disk drive I/O interface 1118, as a boot signal.

In step 1152, the managing controller 1122 provides the computer 1102 with access to the menu area 1126. The computer 1102 retrieves the menu software therefrom, executes it and proceeds to step 1154.

In step 1154, the managing controller 1122 awaits to receive instructions from the user, via the computer 1102, choosing between the various options of modes (i.e. public, secured and the like). At the same time, the managing controller 1122 resets a time counter t. The user is required to provide his selection within a predetermined time period T. If t>T, (i.e. the user did not provide his selection within a predetermined time period T) or the user selects the secured mode, then the managing controller 1122 proceeds to step 1162. Otherwise, the managing controller 1122 proceeds to step 1156.

In step 1156, the managing controller 1122 executes a sequence of operations which determine the public mode, such as enabling access to public devices and denying access to non-public devices, such as secured devices. Accordingly, the managing controller 1122 connects between the public area 1128 and the computer 1102, thus enabling the computer 1102 to load an operating system from the public area 1128. The managing controller further provides communication switch 1142 with a command to connect communication interfaces 1110 and 1112 thus, connecting between the public network 1136 and the computer 1102.

In step 1158, the managing controller 1122 turns on a public data flag and turns off a secured flag. In the present example, both flags are memory elements within managing controller 1122. The public data flag indicates that the current mode is the public mode. The secured data flag indicates that the current mode is the secured mode.

In step 1160, the managing controller detects if the user has provided the computer 1102 with a command to switch to another mode. If so, the managing controller proceeds to step 1168.

In step 1162, the managing controller 1122 executes a sequence of operations which determine the secured mode, such as enabling access to secured devices and denying access to non-secured devices, such as public devices. Accordingly, the managing controller 1122 connects between the secured area 1130 and the computer 1102, thus enabling the computer 1102 to load an operating system from the secured area 1130. The managing controller further provides communication switch 1140 with a command to connect communication interfaces 1114 and 1116 thus, connecting between the secured network 1134 and the computer 1102.

In step 1164, the managing controller 1122 turns on the secured data flag therein and turn off the public flag.

In step 1166, the managing controller detects if the user has provided the computer 1102 with a command to switch to another mode. If so, then the managing controller proceeds to step 1168.

In step 1168, the managing controller 1122 provides an operating system shut-down-restart command to the computer 1102. Accordingly, the computer shuts down all applications as well as the operating system and restarts thereafter. Then, the managing controller 1122 proceeds to step 1170.

In step 1170, the managing controller 1122 resets the computer 1102. According to one aspect of the invention, this reset may be performed by providing a further software boot command to the computer 1102. According to another aspect of the invention, the reset is performed by providing a hardware boot command to the computer 1102. It is noted that, when reset, X86 based PC computers reset most of the RAM except for the first Mbyte of memory, which may include undesired software. According to a further aspect of the invention, the managing controller 1122 provides a reset-all-RAM command to the computer 1102. After executing step 1170, the managing controller 1122 proceeds to step 1172.

In step 1172, the managing controller retrieves the current setting of the security flag and the public flag. If the security flag is turned on and the public flag is turned off, then the managing controller proceeds to step 1156, so as to switch from the secured mode to the public mode. Otherwise, if the security flag is turned off and the public flag is turned on, then the managing controller proceeds to step 1162, so as to switch from the public mode to the secured mode. It is noted that when the system determines more than two modes, such as a plurality of modes which define multi-level, multi-user, multi-client situations, the user is required to provide his mode selection.

Accordingly, the device 1100 can be adapted to support a plurality of multiple level security modes, switching between them and enabling or disabling access to a variety of devices, links and data locations, respectively.

It is noted that in steps 1156 and 1162, after the computer 1102 commences loading the operating system from the chosen area, the managing controller 1122 provides I/O switching unit 1139 with a command to connect between diskette drive input-output (I/O) interfaces 1137 and 1138, thus enabling the computer 1102 to access the diskette drive 1135.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined only by the claims which follow.

What is claimed is:

1. A device for protecting secured areas in a computer system, said computer system comprising a computer and a storage unit, said storage unit including a first storage area and a second storage area, the device comprising:

a first communication interface for connecting to a first network;

a second communication interface for connecting to said computer;

a first input-output (I/O) interface for connecting to said storage unit;

a second input-output (I/O) interface for connecting to said computer; and

a managing controller connected between said first network and said computer via said first and second communication interfaces, said managing controller also being connected between said storage unit and said computer via said first and second I/O interfaces,

said managing controller configured to provide said computer system with a selection between at least two predetermined modes providing non-overlapping physical configurations of said computer system,

wherein, in a first mode, said managing controller connects said computer to said first storage area and to said first network and disconnects said computer from said second storage area, and in a second mode, said managing controller connects said computer to said second storage area and disconnects said computer from said first storage area and from said first network, and

wherein said managing controller detects any reset signal followed by a command to operate according to a selected mode.

2. A device according to claim 1 further comprising:

a third communication interface for connecting to a second network; and

a fourth communication interface for connecting to said computer system;

said device also being connected between said second network and said computer system via said third and fourth communication interfaces,

wherein according to a second mode said managing controller further connects said computer system to said second network.

3. A device according to claim 1 further comprising a display device connected to said managing controller, for providing a visual indication of a current mode.

4. A device according to claim 1 further comprising;

a first reset input-output interface, connected to said managing controller, for connecting to an operating system source unit; and

a second reset input-output interface, connected to said managing controller for connecting to said computer system,

wherein said managing controller controls access of said computer system to said operating system source unit.

5. A device according to claim 4 wherein said operating system source unit is selected from the group consisting of:

a magnetic media drive;

an optical media drive;

an electro-optical media drive;

a communication link; and

a non-volatile memory.

6. A device according to claim 1 wherein said command to operate according to a selected mode is provided to said computer system from a user.

7. A device according to claim 1 wherein said command to operate according to a selected mode is provided to said computer system from a software application.

23

8. A method for operating a communication controlling device, the device connected between a storage unit, a peripheral device and a computer system, the device being operable to provide a first predetermined mode of operation and at least an additional different mode of operation, the method comprising the steps of:

  detecting a boot signal received from said computer system;

  executing a menu procedure;

  receiving an instruction from a user to operate according to a selected mode of operation;

  initiating a reset signal in said computer system;

  entering a listening state; and

  only if said reset signal is detected during said listening state:

    enabling access of said computer system to selected areas of said storage unit according to said selected mode of operation;

    disabling access of said computer system to non-selected areas of said storage unit according to said selected mode of operation;

    enabling access of said computer system to selected areas of said at least one peripheral device, according to said selected mode of operation; and

    disabling access of said computer system to non-selected areas of said peripheral device, according to said selected mode of operation.

9. A method according to claim 8 further comprising the steps of:

  receiving an instruction from a user to operate according to another selected mode of operation;

  providing a restart command to said computer station;

  detecting a boot signal received from said computer station;

  enabling access of said computer station to selected areas of said at least one storage unit according to said other selected mode of operation; and

24

  disabling access of said computer station to non-selected areas of said at least one storage unit according to said other selected mode of operation;

  enabling access of said computer station to selected areas of said at least one peripheral device, according to said other selected mode of operation; and

  disabling access of said computer station to non-selected areas of said at least one peripheral device, according to said other selected mode of operation.

10. A method according to claim 8 further comprising the steps of:

  receiving an instruction from a user to operate according to another selected mode of operation;

  providing a restart command to said computer station;

  detecting a boot signal received from said computer station;

  providing a boot command to said computer station;

  enabling access of said computer station to selected areas of said at least one storage unit according to said other selected mode of operation; and

  disabling access of said computer station to non-selected areas of said at least one storage unit according to said other selected mode of operation;

  enabling access of said computer station to selected areas of said at least one peripheral device, according to said other selected mode of operation; and

  disabling access of said computer station to non-selected areas of said at least one peripheral device, according to said other selected mode of operation.

11. A method according to claim 10 wherein said boot command is a hardware boot command.

12. A method according to claim 10 wherein said boot command is a software boot command.

13. A method according to claim 10 wherein said boot command is followed by resetting the memory of said computer station.

* * * * *